CEL 51, DCCN, Monsoon 2020
Lab 2: Basic Network Utilities

This lab introduces some basic network monitoring/analysis tools. There are a few exercises along the way. You should write up answers to the ***ping*** and ***traceroute*** exercises and turn them in next lab. (You should try out each tool, whether it is needed for an exercise or not!).

Prerequisite: Basic understanding of command line utilities of Linux Operating system.

Some Basic command line Networking utilities

Start with a few of the most basic command line tools. These commands are available on Unix, including Linux (and the first two, at least, are also for Windows). Some parameters or options might differ on different operating systems. Remember that you can use man <command> to get information about a command and its options.

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

Network latency, specifically round trip time (RTT), can be measured using ping, which sends ICMP packets. The syntax for the command in Linux or Mac OS is:

```
ping [-c <count>] [-s <packetsize>] <hostname>
```

The syntax in Windows is:

```
ping [-n <count>] [-l <packetsize>] <hostname>
```

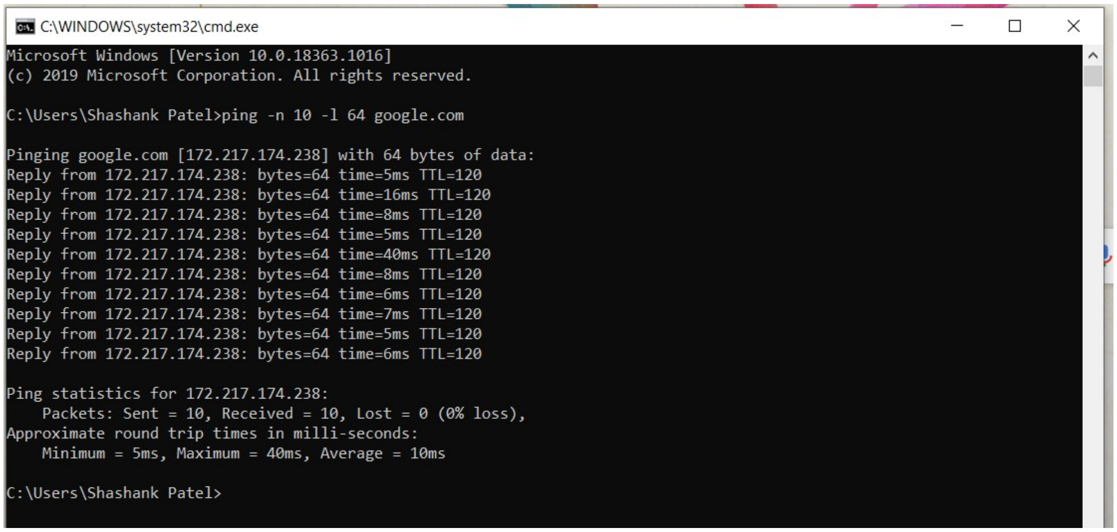
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

```
ping -c 10 google.com > ping_c10_s64_google.log
```

Experiments with Ping

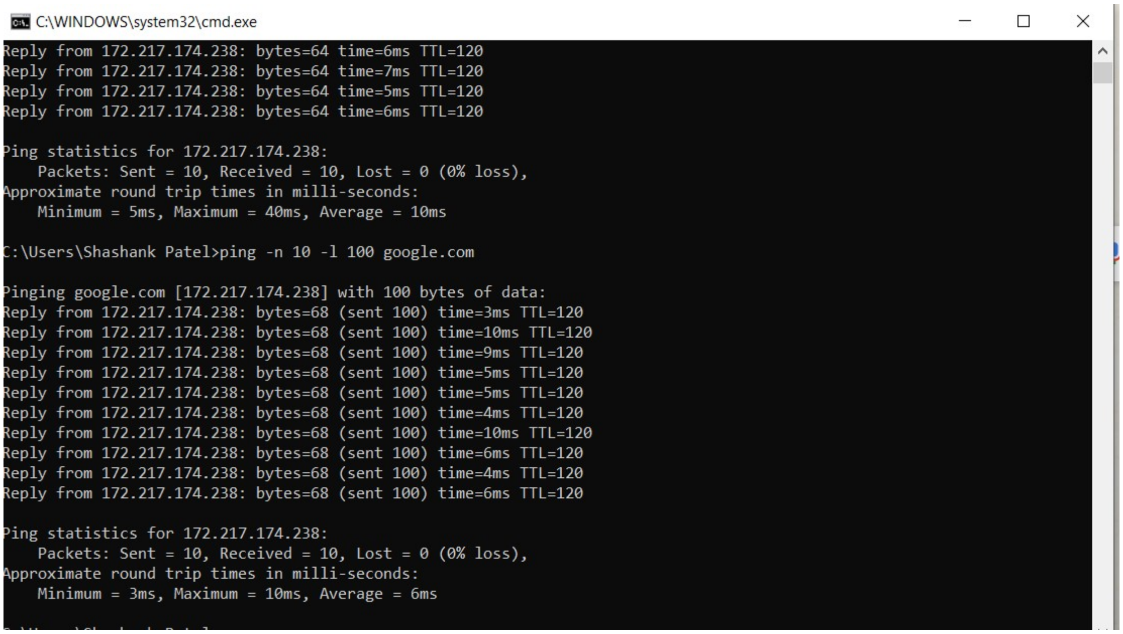
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes



```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Shashank Patel>ping -n 10 -l 64 google.com

Pinging google.com [172.217.174.238] with 64 bytes of data:
Reply from 172.217.174.238: bytes=64 time=5ms TTL=120
Reply from 172.217.174.238: bytes=64 time=16ms TTL=120
Reply from 172.217.174.238: bytes=64 time=8ms TTL=120
Reply from 172.217.174.238: bytes=64 time=5ms TTL=120
Reply from 172.217.174.238: bytes=64 time=40ms TTL=120
Reply from 172.217.174.238: bytes=64 time=8ms TTL=120
Reply from 172.217.174.238: bytes=64 time=6ms TTL=120
Reply from 172.217.174.238: bytes=64 time=7ms TTL=120
Reply from 172.217.174.238: bytes=64 time=5ms TTL=120
Reply from 172.217.174.238: bytes=64 time=6ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 40ms, Average = 10ms

C:\Users\Shashank Patel>
```

Observation:

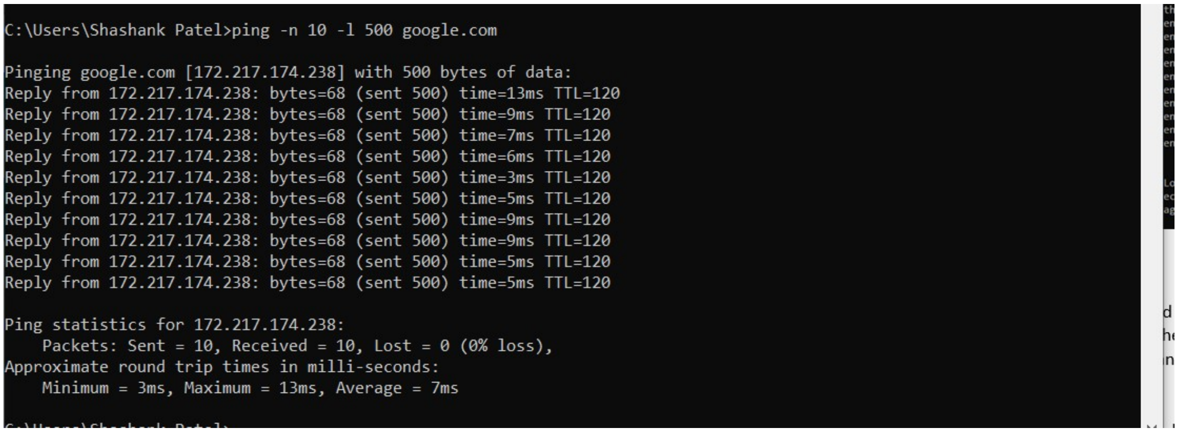
IP address 172.217.174.238 is pinged 10 times with 64 bytes packets when host google.com is pinged. The average RTT is 10 ms.



```
Reply from 172.217.174.238: bytes=64 time=6ms TTL=120
Reply from 172.217.174.238: bytes=64 time=7ms TTL=120
Reply from 172.217.174.238: bytes=64 time=5ms TTL=120
Reply from 172.217.174.238: bytes=64 time=6ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 40ms, Average = 10ms

C:\Users\Shashank Patel>ping -n 10 -l 100 google.com

Pinging google.com [172.217.174.238] with 100 bytes of data:
Reply from 172.217.174.238: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=10ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=10ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=6ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 100) time=6ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 10ms, Average = 6ms
```

Observation:

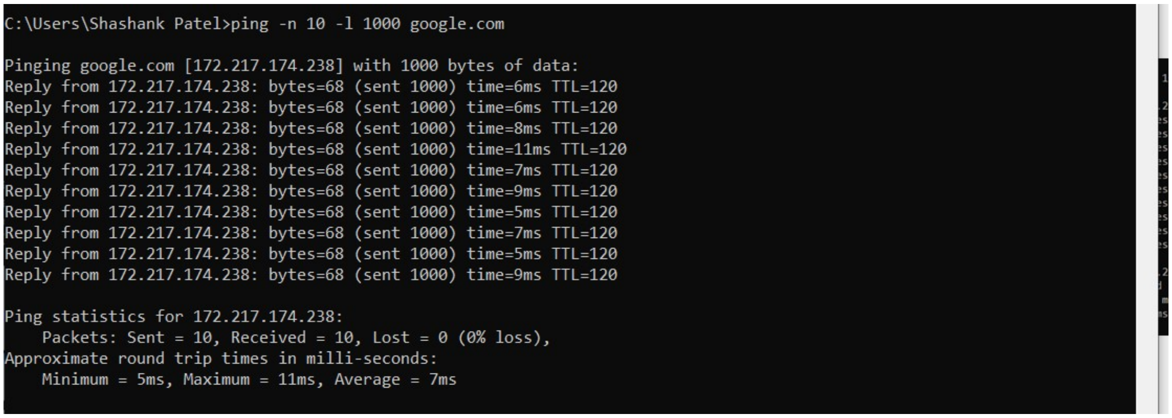
- When google.com is pinged with 10 packets of size 100 bytes, IP address 172.217.174.238 is pinged. This IP address is the same from the previous one.
- The average RTT is less than the previous RTT.



```
C:\Users\Shashank Patel>ping -n 10 -l 500 google.com

Pinging google.com [172.217.174.238] with 500 bytes of data:
Reply from 172.217.174.238: bytes=68 (sent 500) time=13ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=7ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=6ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=3ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 500) time=5ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 13ms, Average = 7ms

C:\Users\Shashank Patel>
```

Observation:

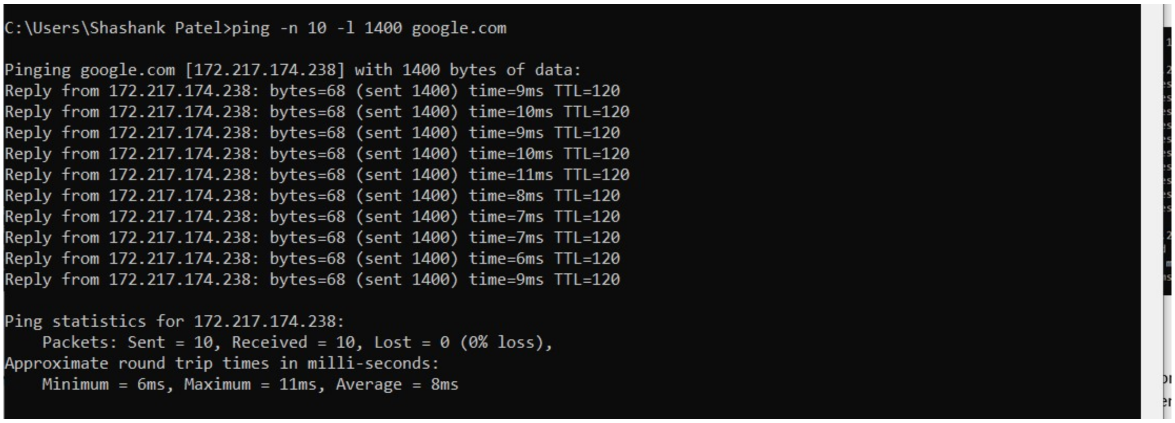
- The avg RTT is 7ms which is more or less same to what the 100 packets sent had.



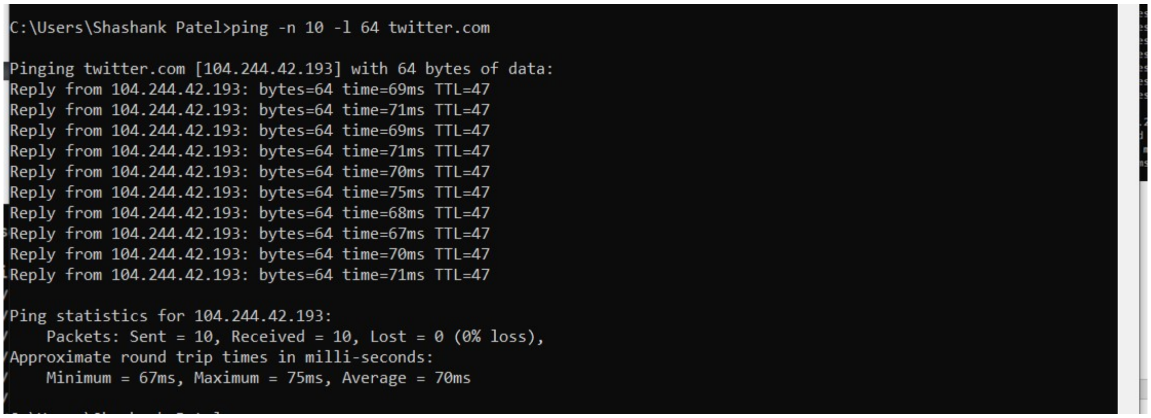
```
C:\Users\Shashank Patel>ping -n 10 -l 1000 google.com

Pinging google.com [172.217.174.238] with 1000 bytes of data:
Reply from 172.217.174.238: bytes=68 (sent 1000) time=6ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=6ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=8ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=11ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=7ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=7ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=5ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1000) time=9ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 11ms, Average = 7ms
```

Observation:

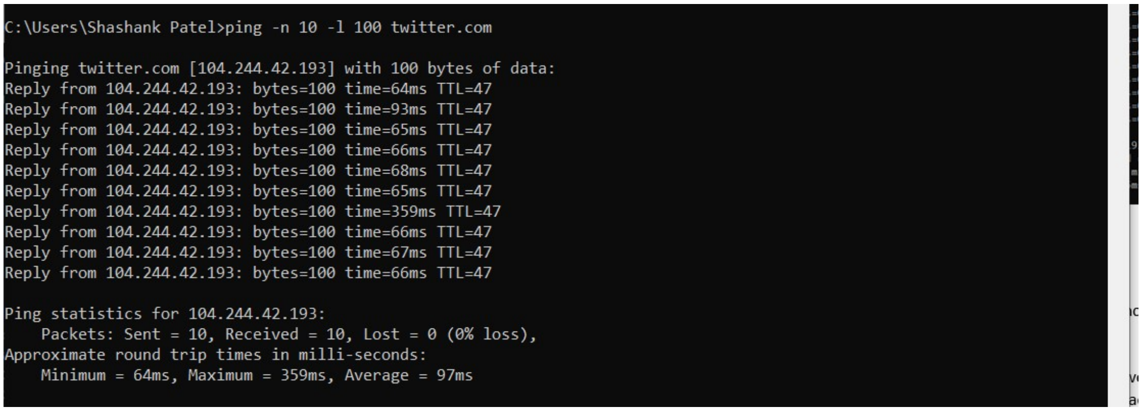
- There is no difference in consecutive packet sizes.



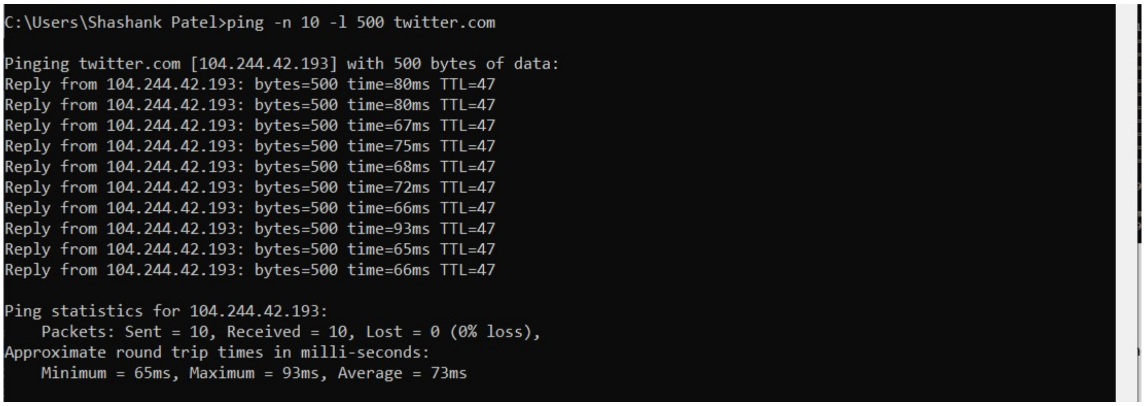
```
C:\Users\Shashank Patel>ping -n 10 -l 1400 google.com

Pinging google.com [172.217.174.238] with 1400 bytes of data:
Reply from 172.217.174.238: bytes=68 (sent 1400) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=10ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=9ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=10ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=11ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=8ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=7ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=7ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=6ms TTL=120
Reply from 172.217.174.238: bytes=68 (sent 1400) time=9ms TTL=120

Ping statistics for 172.217.174.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 11ms, Average = 8ms
```



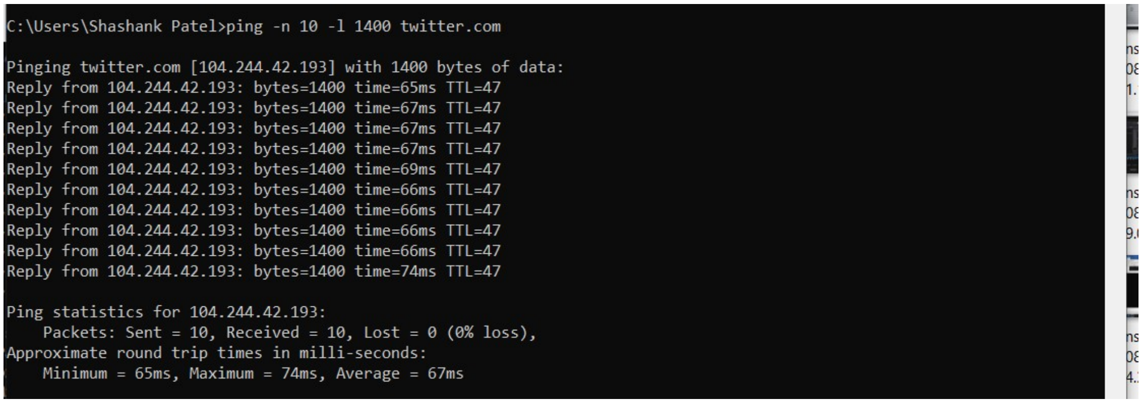
```
C:\Users\Shashank Patel>ping -n 10 -l 64 twitter.com

Pinging twitter.com [104.244.42.193] with 64 bytes of data:
Reply from 104.244.42.193: bytes=64 time=69ms TTL=47
Reply from 104.244.42.193: bytes=64 time=71ms TTL=47
Reply from 104.244.42.193: bytes=64 time=69ms TTL=47
Reply from 104.244.42.193: bytes=64 time=71ms TTL=47
Reply from 104.244.42.193: bytes=64 time=70ms TTL=47
Reply from 104.244.42.193: bytes=64 time=75ms TTL=47
Reply from 104.244.42.193: bytes=64 time=68ms TTL=47
Reply from 104.244.42.193: bytes=64 time=67ms TTL=47
Reply from 104.244.42.193: bytes=64 time=70ms TTL=47
Reply from 104.244.42.193: bytes=64 time=71ms TTL=47

Ping statistics for 104.244.42.193:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 75ms, Average = 70ms
```



```
C:\Users\Shashank Patel>ping -n 10 -l 100 twitter.com

Pinging twitter.com [104.244.42.193] with 100 bytes of data:
Reply from 104.244.42.193: bytes=100 time=64ms TTL=47
Reply from 104.244.42.193: bytes=100 time=93ms TTL=47
Reply from 104.244.42.193: bytes=100 time=65ms TTL=47
Reply from 104.244.42.193: bytes=100 time=66ms TTL=47
Reply from 104.244.42.193: bytes=100 time=68ms TTL=47
Reply from 104.244.42.193: bytes=100 time=65ms TTL=47
Reply from 104.244.42.193: bytes=100 time=359ms TTL=47
Reply from 104.244.42.193: bytes=100 time=66ms TTL=47
Reply from 104.244.42.193: bytes=100 time=67ms TTL=47
Reply from 104.244.42.193: bytes=100 time=66ms TTL=47

Ping statistics for 104.244.42.193:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 359ms, Average = 97ms
```



```
C:\Users\Shashank Patel>ping -n 10 -l 500 twitter.com

Pinging twitter.com [104.244.42.193] with 500 bytes of data:
Reply from 104.244.42.193: bytes=500 time=80ms TTL=47
Reply from 104.244.42.193: bytes=500 time=80ms TTL=47
Reply from 104.244.42.193: bytes=500 time=67ms TTL=47
Reply from 104.244.42.193: bytes=500 time=75ms TTL=47
Reply from 104.244.42.193: bytes=500 time=68ms TTL=47
Reply from 104.244.42.193: bytes=500 time=72ms TTL=47
Reply from 104.244.42.193: bytes=500 time=66ms TTL=47
Reply from 104.244.42.193: bytes=500 time=93ms TTL=47
Reply from 104.244.42.193: bytes=500 time=65ms TTL=47
Reply from 104.244.42.193: bytes=500 time=66ms TTL=47

Ping statistics for 104.244.42.193:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 93ms, Average = 73ms
```



```
C:\Users\Shashank Patel>ping -n 10 -l 1400 twitter.com

Pinging twitter.com [104.244.42.193] with 1400 bytes of data:
Reply from 104.244.42.193: bytes=1400 time=65ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=67ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=67ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=67ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=69ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=66ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=66ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=66ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=66ms TTL=47
Reply from 104.244.42.193: bytes=1400 time=74ms TTL=47

Ping statistics for 104.244.42.193:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 74ms, Average = 67ms
```

QUESTIONS ABOUT LATENCY

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named ping.txt.

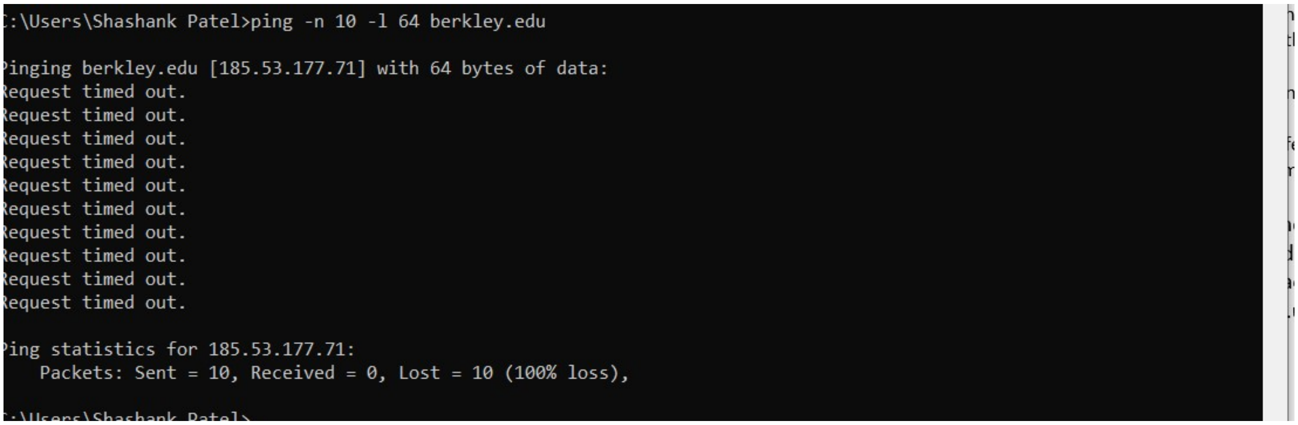
1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

   Ans. Yes, RTT vary between different hosts. The physical path through which the packets transmit do matter as faster paths like fibre optic cables can do the job much faster. Also the distance to be travelled i.e the propagation affects as larger the distance more time it takes to propagate. More the queuing delay in a packet switched network more time the packet would take to reach the receiver.

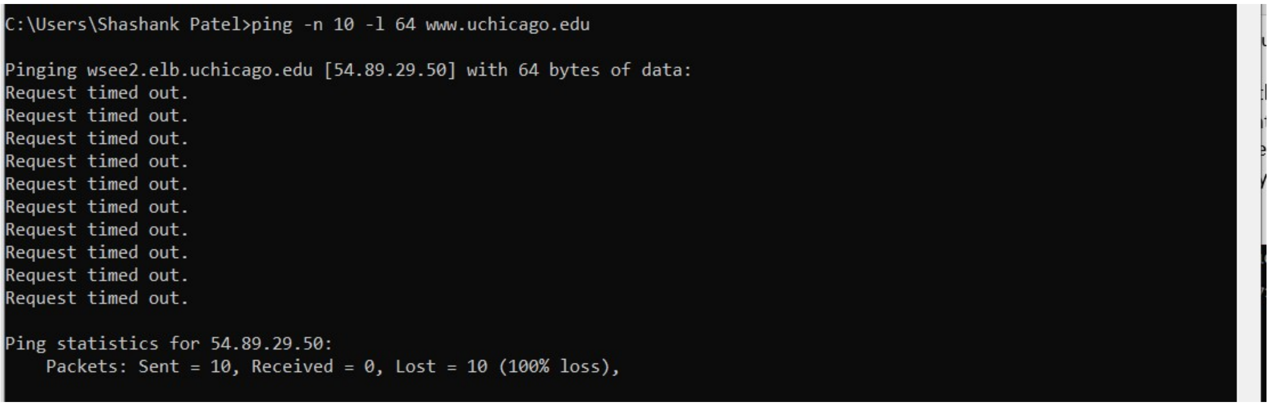
2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

   Ans. Yes, RTT varies with packet sizes. This reason would be the bandwidth of the internet connection. Higher the bandwidth lower is the RTT. Also transmit and propagation increases time as more data is to be sent by the sender.

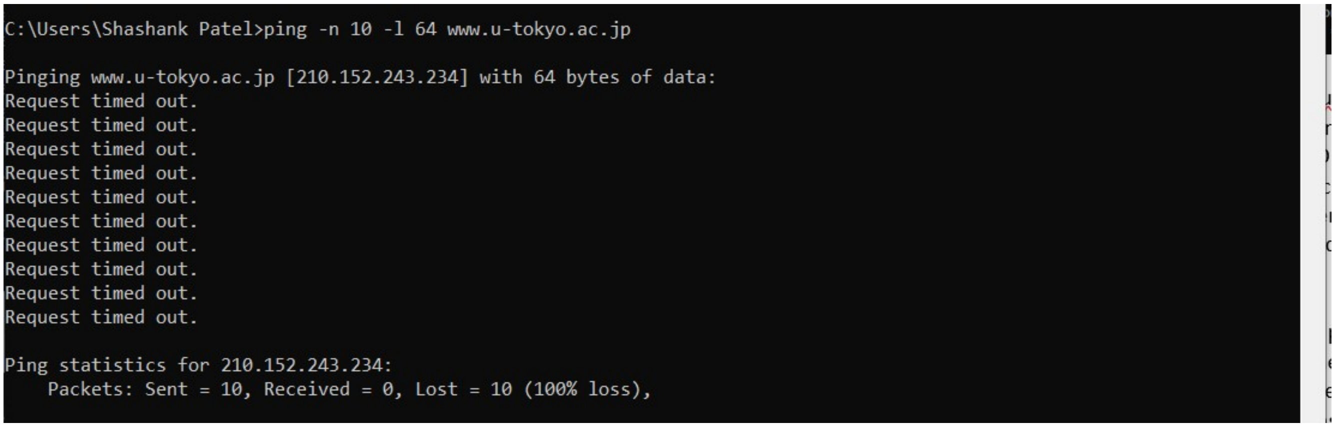
Exercise 1: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).



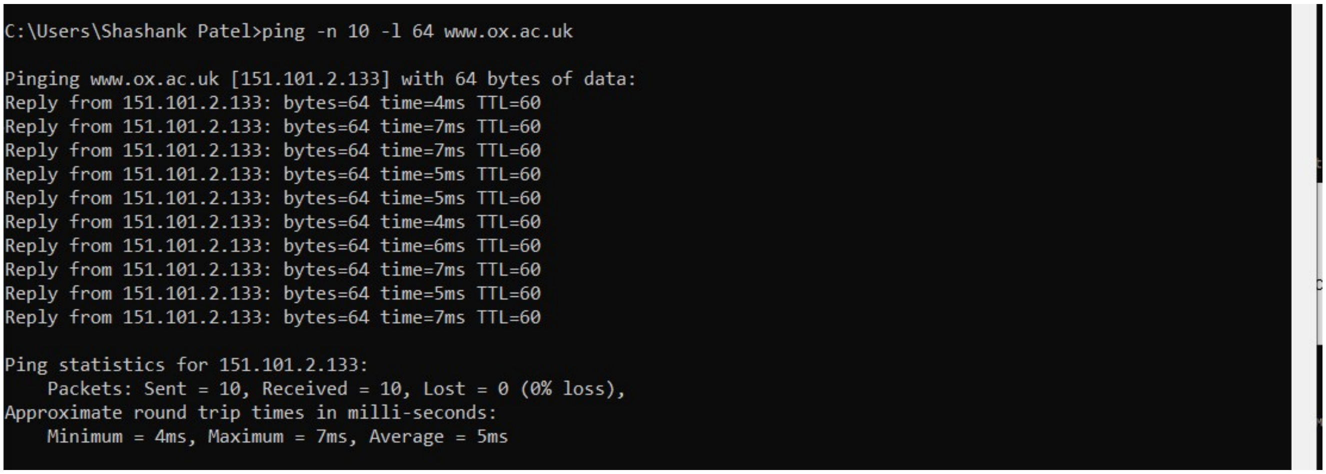
```
C:\Users\Shashank Patel>ping -n 10 -l 64 berkley.edu

Pinging berkley.edu [185.53.177.71] with 64 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 185.53.177.71:
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),

C:\Users\Shashank Patel>
```



```
C:\Users\Shashank Patel>ping -n 10 -l 64 www.uchicago.edu

Pinging wsee2.elb.uchicago.edu [54.89.29.50] with 64 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 54.89.29.50:
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),
```



```
C:\Users\Shashank Patel>ping -n 10 -l 64 www.u-tokyo.ac.jp

Pinging www.u-tokyo.ac.jp [210.152.243.234] with 64 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 210.152.243.234:
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),
```



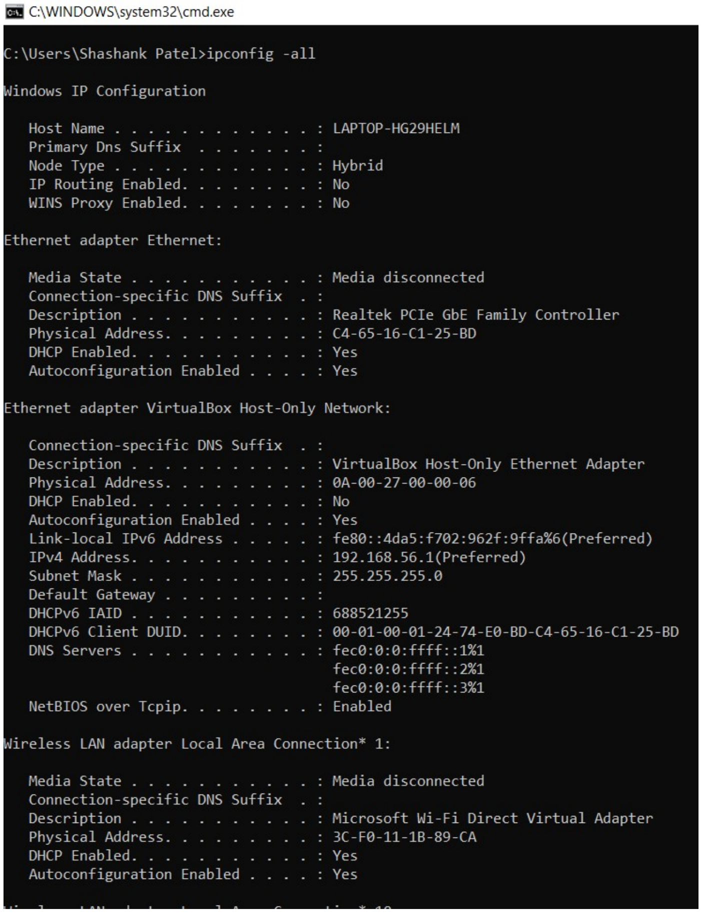
```
C:\Users\Shashank Patel>ping -n 10 -l 64 www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.2.133] with 64 bytes of data:
Reply from 151.101.2.133: bytes=64 time=4ms TTL=60
Reply from 151.101.2.133: bytes=64 time=7ms TTL=60
Reply from 151.101.2.133: bytes=64 time=7ms TTL=60
Reply from 151.101.2.133: bytes=64 time=5ms TTL=60
Reply from 151.101.2.133: bytes=64 time=5ms TTL=60
Reply from 151.101.2.133: bytes=64 time=4ms TTL=60
Reply from 151.101.2.133: bytes=64 time=6ms TTL=60
Reply from 151.101.2.133: bytes=64 time=7ms TTL=60
Reply from 151.101.2.133: bytes=64 time=5ms TTL=60
Reply from 151.101.2.133: bytes=64 time=7ms TTL=60

Ping statistics for 151.101.2.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

Observation:

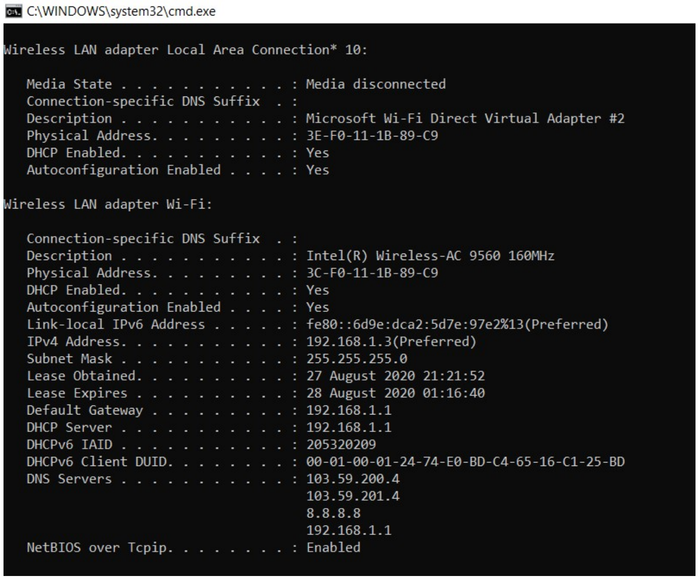
The RTT for different hosts can be different. It varies on the basis of propagation and the transmission media used primarily.

nslookup — The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslokup by adding the server name or IP address to the command: nslookup <host> <server>

ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!!.)

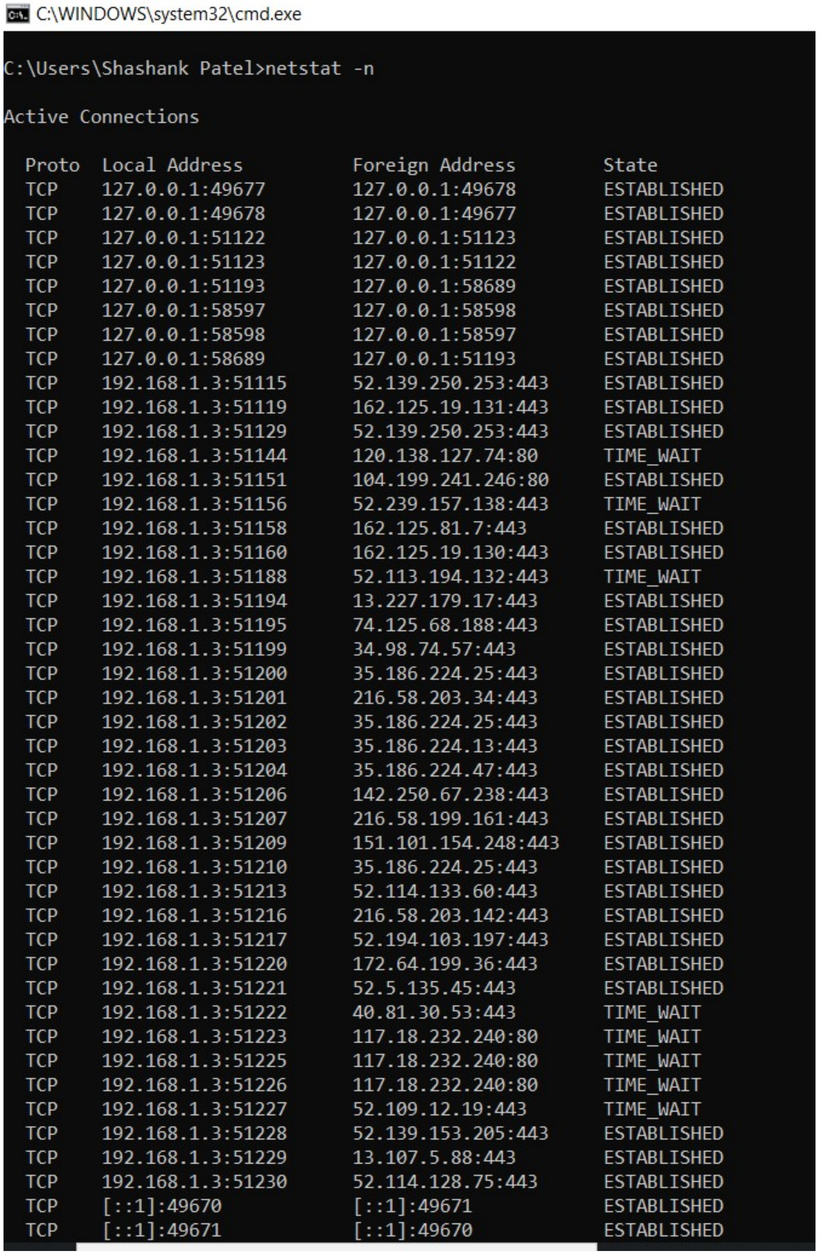


```
C:\Users\Shashank Patel>ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-HG29HELM
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : C4-65-16-C1-25-BD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-06
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4da5:f702:962f:9ffa%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 688521255
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-74-E0-BD-C4-65-16-C1-25-BD
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 3C-F0-11-1B-89-CA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:
```



```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 3E-F0-11-1B-89-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 3C-F0-11-1B-89-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6d9e:dca2:5d7e:97e2%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 27 August 2020 21:21:52
   Lease Expires . . . . . . . . . . : 28 August 2020 01:16:40
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 205320209
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-74-E0-BD-C4-65-16-C1-25-BD
   DNS Servers . . . . . . . . . . . : 103.59.200.4
                                       103.59.201.4
                                       8.8.8.8
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)



C:\WINDOWS\system32\cmd.exe

```
C:\Users\Shashank Patel>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49677        127.0.0.1:49678        ESTABLISHED
  TCP    127.0.0.1:49678        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:51122        127.0.0.1:51123        ESTABLISHED
  TCP    127.0.0.1:51123        127.0.0.1:51122        ESTABLISHED
  TCP    127.0.0.1:51193        127.0.0.1:58689        ESTABLISHED
  TCP    127.0.0.1:58597        127.0.0.1:58598        ESTABLISHED
  TCP    127.0.0.1:58598        127.0.0.1:58597        ESTABLISHED
  TCP    127.0.0.1:58689        127.0.0.1:51193        ESTABLISHED
  TCP    192.168.1.3:51115      52.139.250.253:443     ESTABLISHED
  TCP    192.168.1.3:51119      162.125.19.131:443     ESTABLISHED
  TCP    192.168.1.3:51129      52.139.250.253:443     ESTABLISHED
  TCP    192.168.1.3:51144      120.138.127.74:80      TIME_WAIT
  TCP    192.168.1.3:51151      104.199.241.246:80     ESTABLISHED
  TCP    192.168.1.3:51156      52.239.157.138:443     TIME_WAIT
  TCP    192.168.1.3:51158      162.125.81.7:443       ESTABLISHED
  TCP    192.168.1.3:51160      162.125.19.130:443     ESTABLISHED
  TCP    192.168.1.3:51188      52.113.194.132:443     TIME_WAIT
  TCP    192.168.1.3:51194      13.227.179.17:443      ESTABLISHED
  TCP    192.168.1.3:51195      74.125.68.188:443      ESTABLISHED
  TCP    192.168.1.3:51199      34.98.74.57:443        ESTABLISHED
  TCP    192.168.1.3:51200      35.186.224.25:443      ESTABLISHED
  TCP    192.168.1.3:51201      216.58.203.34:443      ESTABLISHED
  TCP    192.168.1.3:51202      35.186.224.25:443      ESTABLISHED
  TCP    192.168.1.3:51203      35.186.224.13:443      ESTABLISHED
  TCP    192.168.1.3:51204      35.186.224.47:443      ESTABLISHED
  TCP    192.168.1.3:51206      142.250.67.238:443     ESTABLISHED
  TCP    192.168.1.3:51207      216.58.199.161:443     ESTABLISHED
  TCP    192.168.1.3:51209      151.101.154.248:443    ESTABLISHED
  TCP    192.168.1.3:51210      35.186.224.25:443      ESTABLISHED
  TCP    192.168.1.3:51213      52.114.133.60:443      ESTABLISHED
  TCP    192.168.1.3:51216      216.58.203.142:443     ESTABLISHED
  TCP    192.168.1.3:51217      52.194.103.197:443     ESTABLISHED
  TCP    192.168.1.3:51220      172.64.199.36:443      ESTABLISHED
  TCP    192.168.1.3:51221      52.5.135.45:443        ESTABLISHED
  TCP    192.168.1.3:51222      40.81.30.53:443        TIME_WAIT
  TCP    192.168.1.3:51223      117.18.232.240:80      TIME_WAIT
  TCP    192.168.1.3:51225      117.18.232.240:80      TIME_WAIT
  TCP    192.168.1.3:51226      117.18.232.240:80      TIME_WAIT
  TCP    192.168.1.3:51227      52.109.12.19:443       TIME_WAIT
  TCP    192.168.1.3:51228      52.139.153.205:443     ESTABLISHED
  TCP    192.168.1.3:51229      13.107.5.88:443        ESTABLISHED
  TCP    192.168.1.3:51230      52.114.128.75:443      ESTABLISHED
  TCP    [::1]:49670            [::1]:49671            ESTABLISHED
  TCP    [::1]:49671            [::1]:49670            ESTABLISHED
```

telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telent <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

traceroute — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ... away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute

The path taken through a network, can be measured using traceroute. The syntax for the command in Linux is:

```
traceroute <hostname>
```

The syntax in Windows is:

```
tracert <hostname>
```

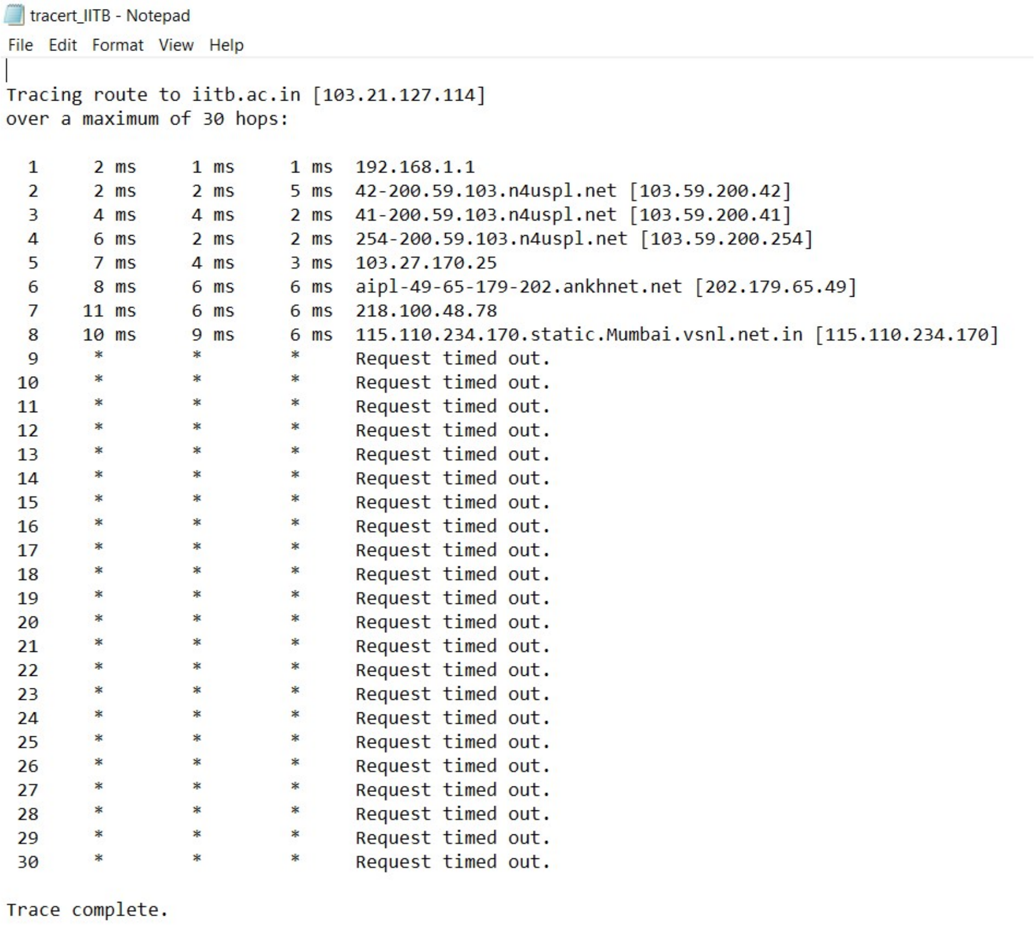
You can specify either a hostname (e.g., cs.iitb.ac.in) or an IP address (e.g., 128.105.2.6).

1.2.1 Experiments with Traceroute

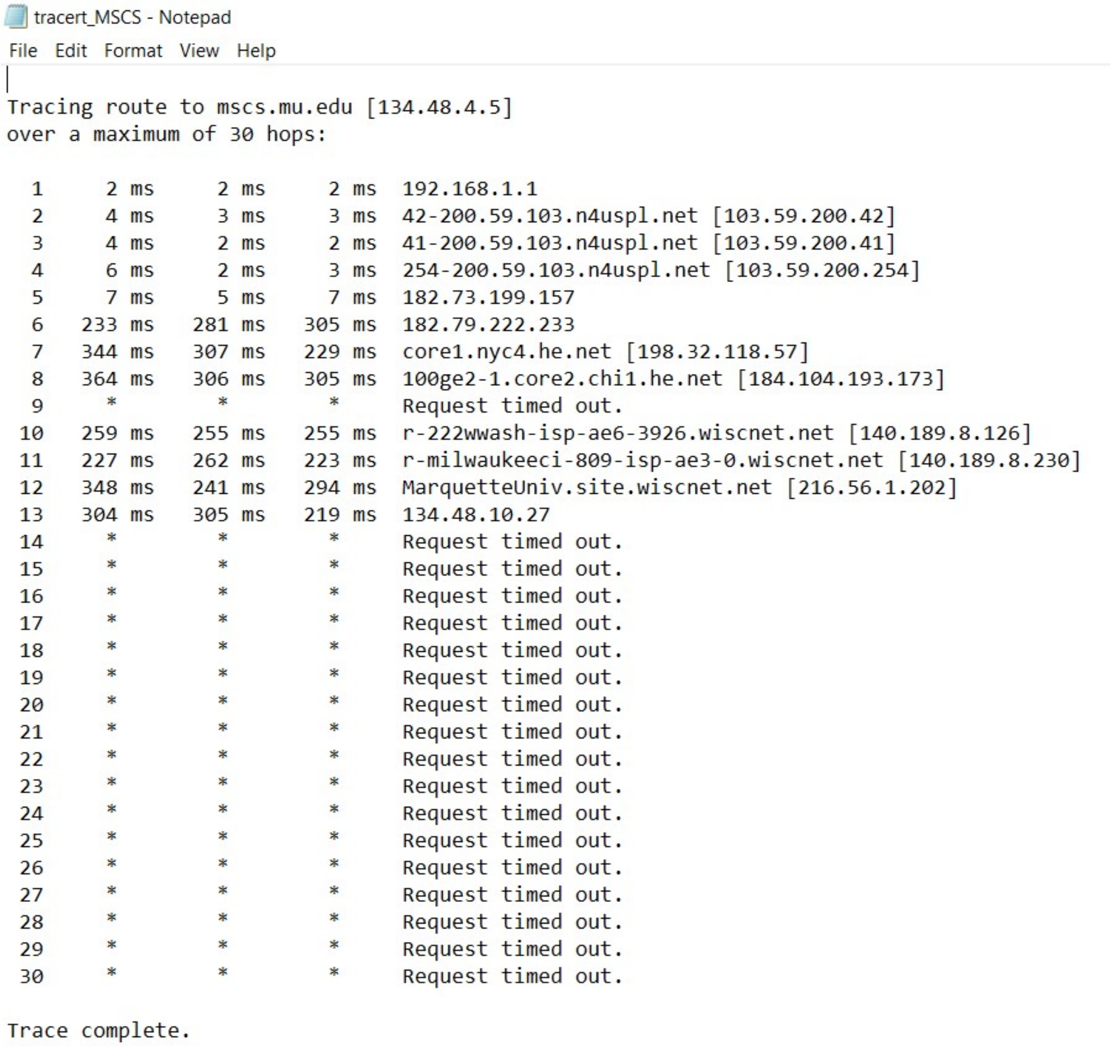
From **your machine** traceroute to the following hosts:

1. ee.iitb.ac.in
2. mscs.mu.edu
3. www.cs.grinnell.edu
4. csail.mit.edu
5. cs.stanford.edu
6. cs.manchester.ac.uk

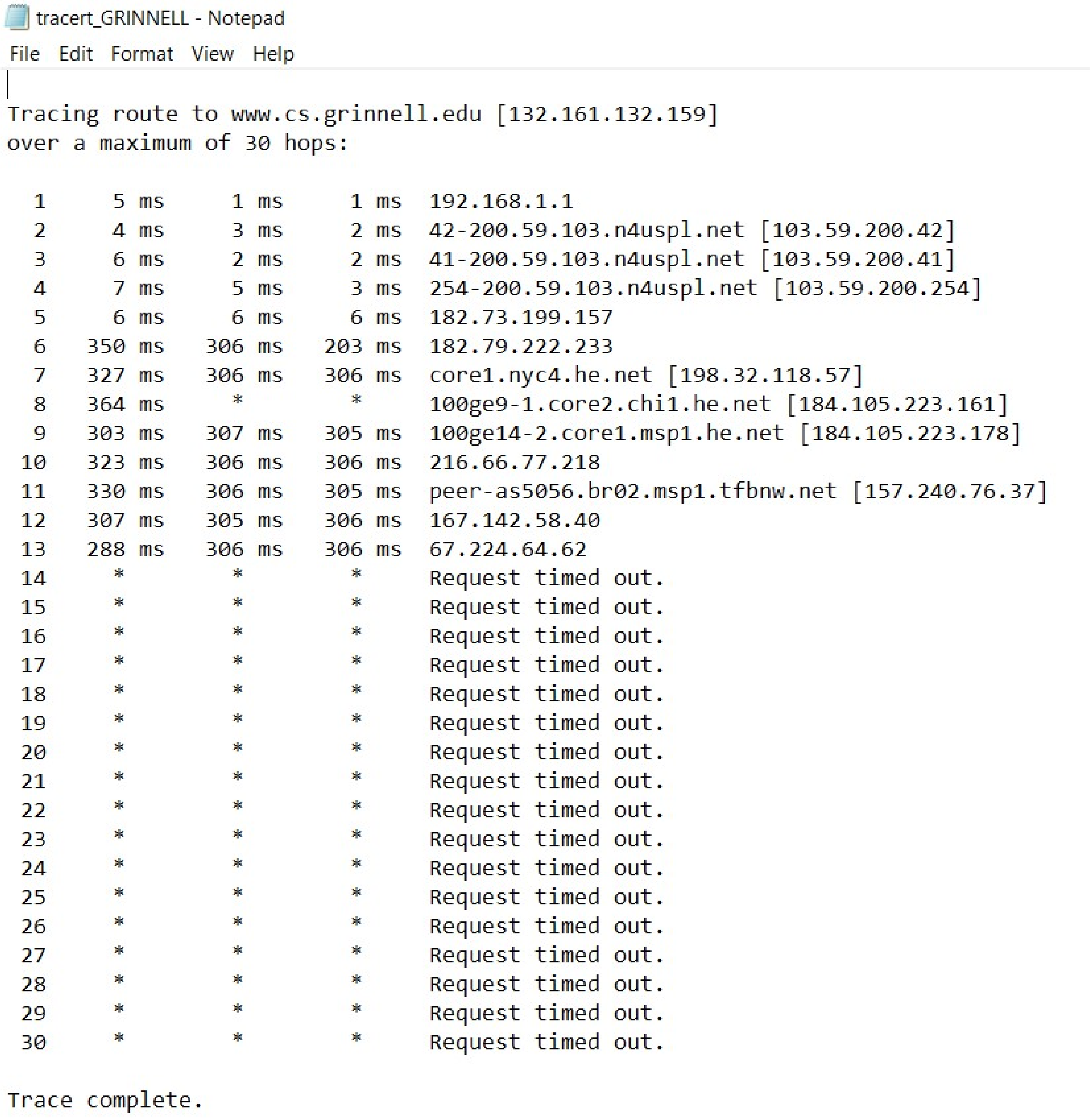
Store the output of each traceroute command in a separate file named traceroute_HOSTNAME.log, replacing HOSTNAME with the hostname for end-host you pinged (e.g., traceroute_ee.iitb.ac.in.log).



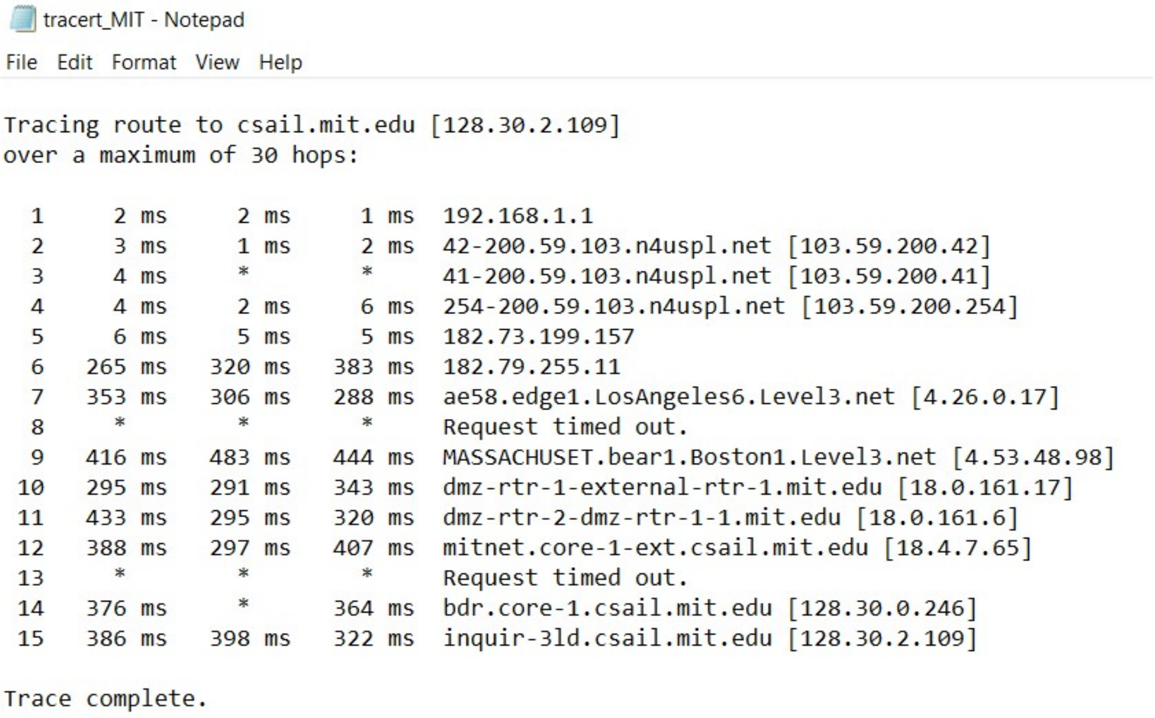
```
Tracing route to iitb.ac.in [103.21.127.114]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2     2 ms     2 ms     5 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     4 ms     4 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     6 ms     2 ms     2 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     7 ms     4 ms     3 ms  103.27.170.25
  6     8 ms     6 ms     6 ms  aipl-49-65-179-202.ankhnet.net [202.179.65.49]
  7    11 ms     6 ms     6 ms  218.100.48.78
  8    10 ms     9 ms     6 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



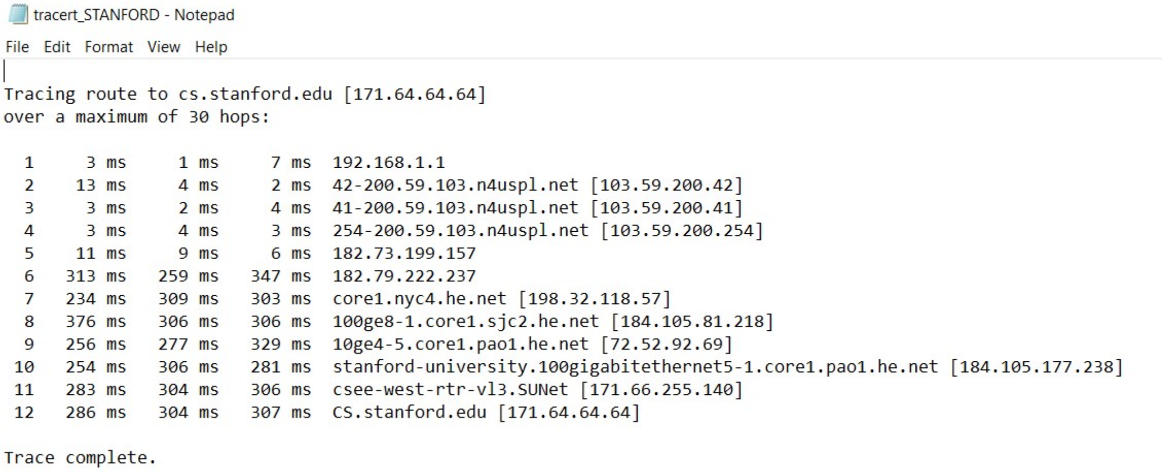
```
Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.1.1
  2     4 ms     3 ms     3 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     4 ms     2 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     6 ms     2 ms     3 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     7 ms     5 ms     7 ms  182.73.199.157
  6   233 ms   281 ms   305 ms  182.79.222.233
  7   344 ms   307 ms   229 ms  core1.nyc4.he.net [198.32.118.57]
  8   364 ms   306 ms   305 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
  9     *        *        *     Request timed out.
 10   259 ms   255 ms   255 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 11   227 ms   262 ms   223 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 12   348 ms   241 ms   294 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 13   304 ms   305 ms   219 ms  134.48.10.27
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



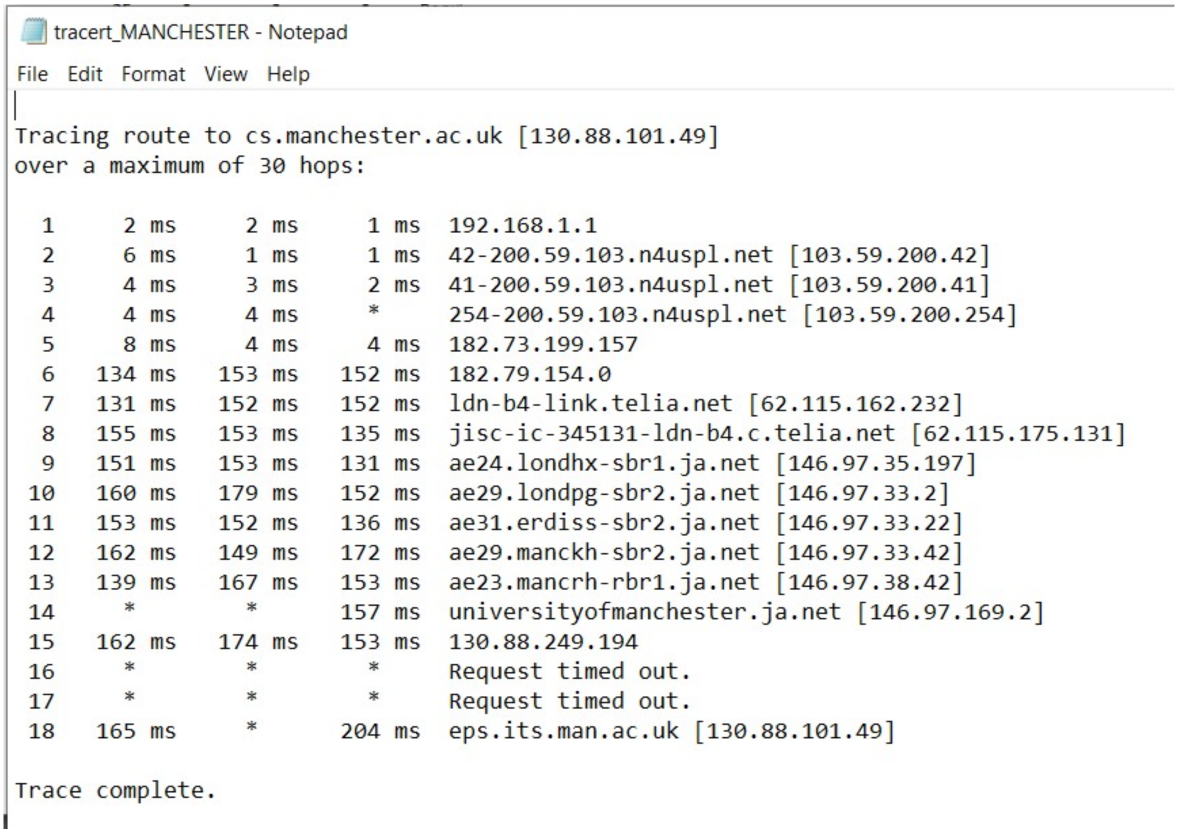
```
Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

  1     5 ms     1 ms     1 ms  192.168.1.1
  2     4 ms     3 ms     2 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     6 ms     2 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     7 ms     5 ms     3 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     6 ms     6 ms     6 ms  182.73.199.157
  6   350 ms   306 ms   203 ms  182.79.222.233
  7   327 ms   306 ms   306 ms  core1.nyc4.he.net [198.32.118.57]
  8   364 ms     *        *     100ge9-1.core2.chi1.he.net [184.105.223.161]
  9   303 ms   307 ms   305 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 10   323 ms   306 ms   306 ms  216.66.77.218
 11   330 ms   306 ms   305 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 12   307 ms   305 ms   306 ms  167.142.58.40
 13   288 ms   306 ms   306 ms  67.224.64.62
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



```
Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.1.1
  2     3 ms     1 ms     2 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     4 ms     *        *     41-200.59.103.n4uspl.net [103.59.200.41]
  4     4 ms     2 ms     6 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     6 ms     5 ms     5 ms  182.73.199.157
  6   265 ms   320 ms   383 ms  182.79.255.11
  7   353 ms   306 ms   288 ms  ae58.edge1.LosAngeles6.Level3.net [4.26.0.17]
  8     *        *        *     Request timed out.
  9   416 ms   483 ms   444 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 10   295 ms   291 ms   343 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 11   433 ms   295 ms   320 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 12   388 ms   297 ms   407 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 13     *        *        *     Request timed out.
 14   376 ms     *      364 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 15   386 ms   398 ms   322 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

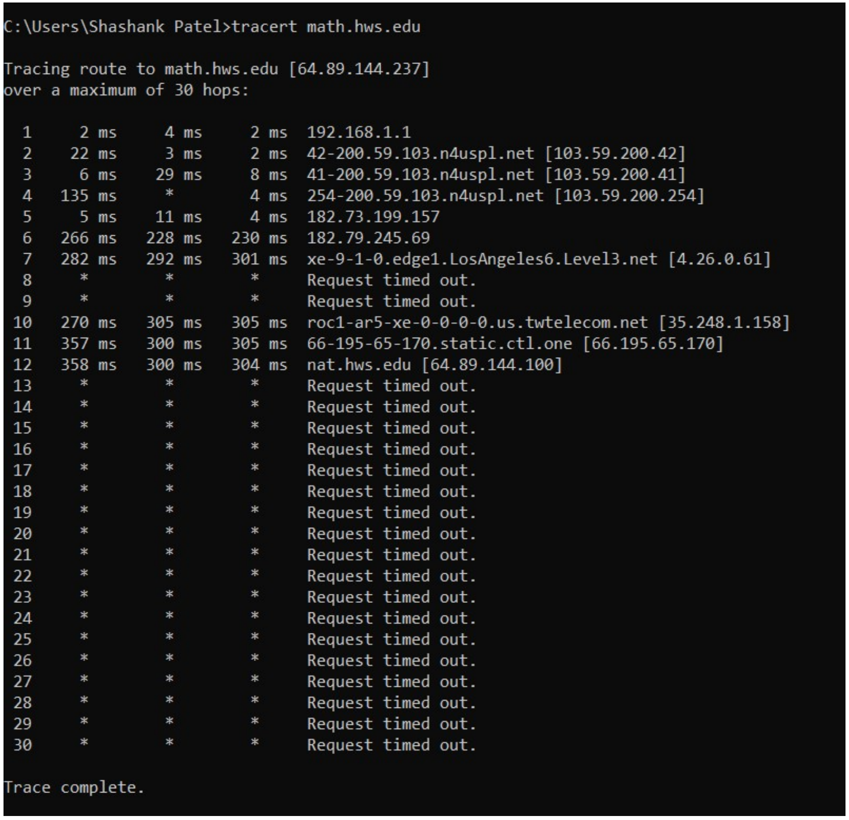


```
Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     3 ms     1 ms     7 ms  192.168.1.1
  2    13 ms     4 ms     2 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     3 ms     2 ms     4 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     3 ms     4 ms     3 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5    11 ms     9 ms     6 ms  182.73.199.157
  6   313 ms   259 ms   347 ms  182.79.222.237
  7   234 ms   309 ms   303 ms  core1.nyc4.he.net [198.32.118.57]
  8   376 ms   306 ms   306 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9   256 ms   277 ms   329 ms  10ge4-5.core1.pao1.he.net [72.52.92.69]
 10   254 ms   306 ms   281 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11   283 ms   304 ms   306 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12   286 ms   304 ms   307 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

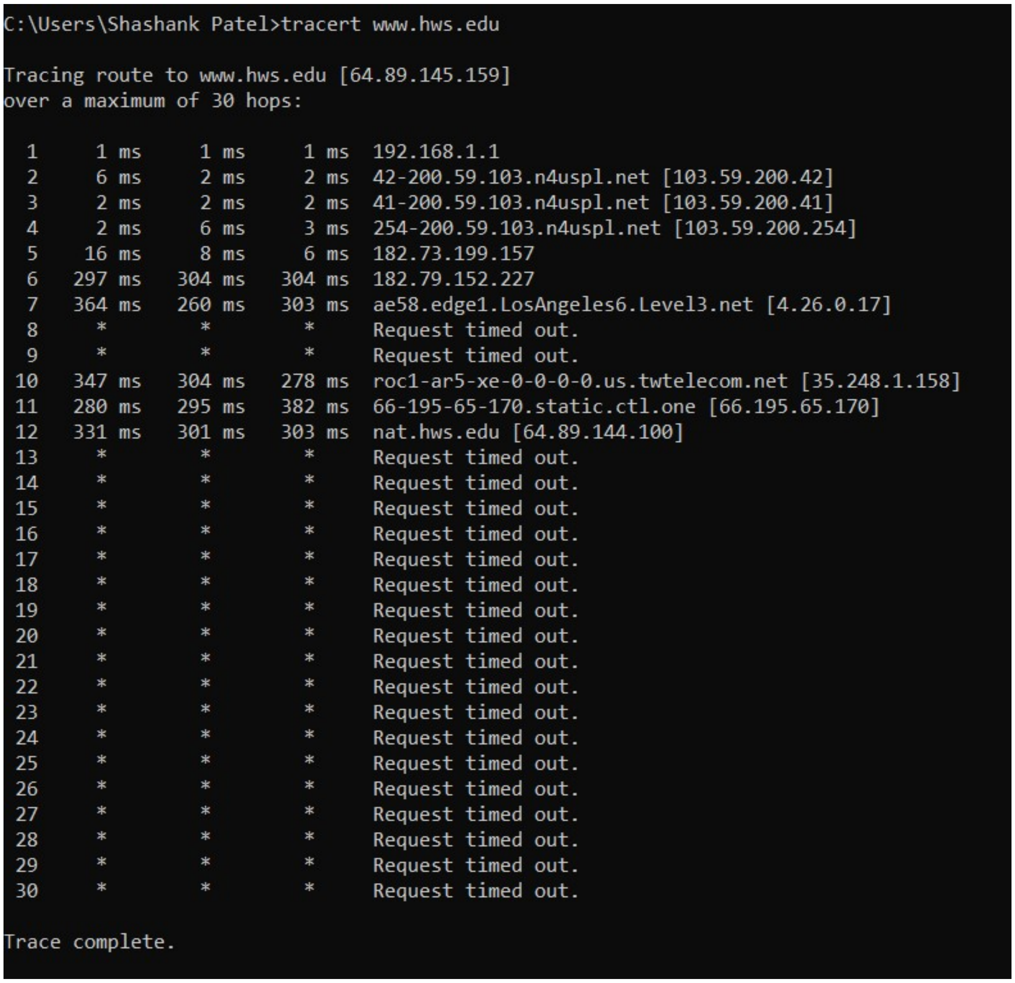


```
Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.1.1
  2     6 ms     1 ms     1 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     4 ms     3 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     4 ms     4 ms     *     254-200.59.103.n4uspl.net [103.59.200.254]
  5     8 ms     4 ms     4 ms  182.73.199.157
  6   134 ms   153 ms   152 ms  182.79.154.0
  7   131 ms   152 ms   152 ms  ldn-b4-link.telia.net [62.115.162.232]
  8   155 ms   153 ms   135 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
  9   151 ms   153 ms   131 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 10   160 ms   179 ms   152 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 11   153 ms   152 ms   136 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 12   162 ms   149 ms   172 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 13   139 ms   167 ms   153 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14     *        *      157 ms  universityofmanchester.ja.net [146.97.169.2]
 15   162 ms   174 ms   153 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18   165 ms     *      204 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

<u>Exercise 2:</u> (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.



```
C:\Users\Shashank Patel>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1     2 ms     4 ms     2 ms  192.168.1.1
  2    22 ms     3 ms     2 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     6 ms    29 ms     8 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4   135 ms     *        4 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     5 ms    11 ms     4 ms  182.73.199.157
  6   266 ms   228 ms   230 ms  182.79.245.69
  7   282 ms   292 ms   301 ms  xe-9-1-0.edge1.LosAngeles6.Level3.net [4.26.0.61]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   270 ms   305 ms   305 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   357 ms   300 ms   305 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   358 ms   300 ms   304 ms  nat.hws.edu [64.89.144.100]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

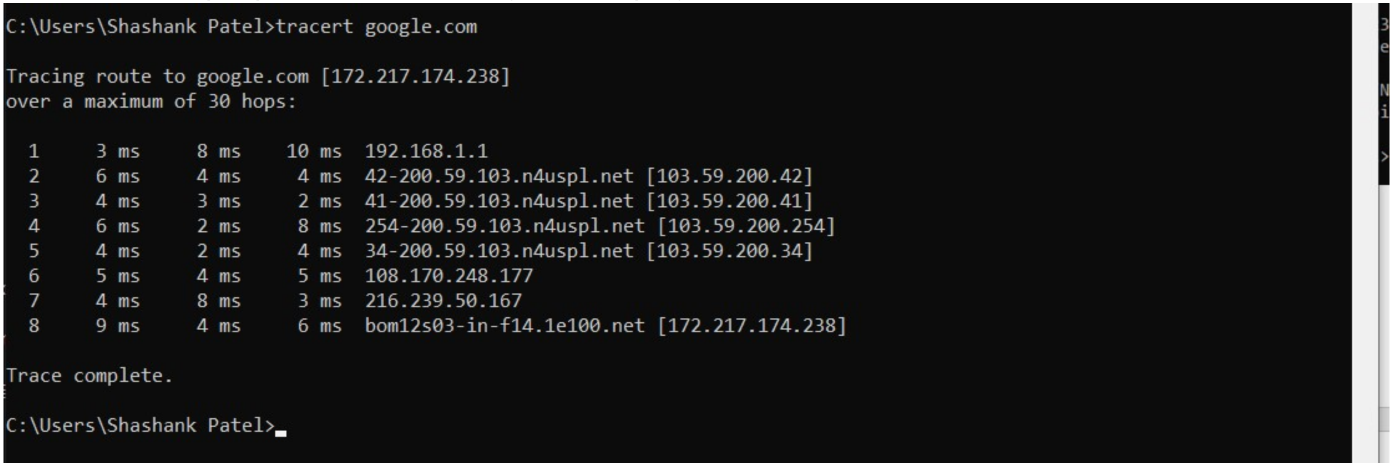


```
C:\Users\Shashank Patel>tracert www.hws.edu

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     6 ms     2 ms     2 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     2 ms     2 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     2 ms     6 ms     3 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5    16 ms     8 ms     6 ms  182.73.199.157
  6   297 ms   304 ms   304 ms  182.79.152.227
  7   364 ms   260 ms   303 ms  ae58.edge1.LosAngeles6.Level3.net [4.26.0.17]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   347 ms   304 ms   278 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   280 ms   295 ms   382 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   331 ms   301 ms   303 ms  nat.hws.edu [64.89.144.100]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Observation:
From the above result we see that the path followed by the route is the same and after the 12th hop both routes display request timed out.

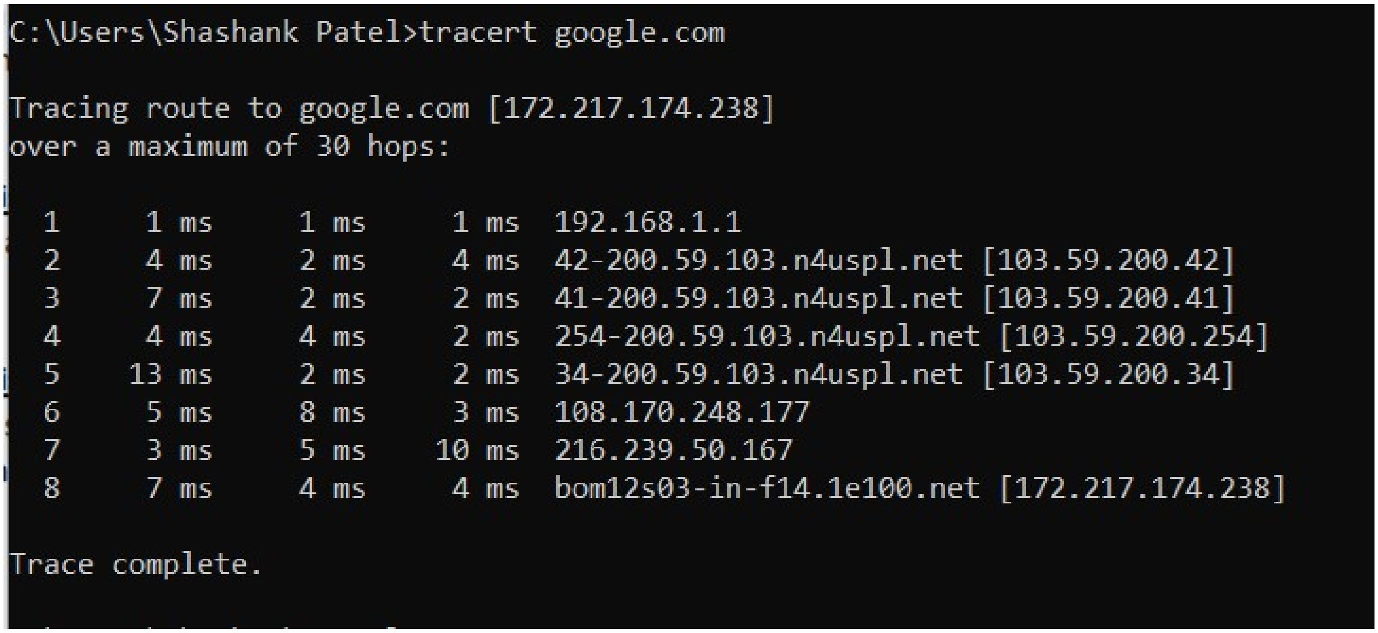
<u>Exercise 3:</u> Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week, try the same destinations again, and compare the results with the results from today. Report your observations.

Trace route on google.com on Thursday, 28th Aug, 1pm



```
C:\Users\Shashank Patel>tracert google.com

Tracing route to google.com [172.217.174.238]
over a maximum of 30 hops:

  1     3 ms     8 ms    10 ms  192.168.1.1
  2     6 ms     4 ms     4 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     4 ms     3 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     6 ms     2 ms     8 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5     4 ms     2 ms     4 ms  34-200.59.103.n4uspl.net [103.59.200.34]
  6     5 ms     4 ms     5 ms  108.170.248.177
  7     4 ms     8 ms     3 ms  216.239.50.167
  8     9 ms     4 ms     6 ms  bom12s03-in-f14.1e100.net [172.217.174.238]

Trace complete.

C:\Users\Shashank Patel>
```

Trace route on google.com on Thursday, 28th Aug, 3pm



```
C:\Users\Shashank Patel>tracert google.com

Tracing route to google.com [172.217.174.238]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     4 ms     2 ms     4 ms  42-200.59.103.n4uspl.net [103.59.200.42]
  3     7 ms     2 ms     2 ms  41-200.59.103.n4uspl.net [103.59.200.41]
  4     4 ms     4 ms     2 ms  254-200.59.103.n4uspl.net [103.59.200.254]
  5    13 ms     2 ms     2 ms  34-200.59.103.n4uspl.net [103.59.200.34]
  6     5 ms     8 ms     3 ms  108.170.248.177
  7     3 ms     5 ms    10 ms  216.239.50.167
  8     7 ms     4 ms     4 ms  bom12s03-in-f14.1e100.net [172.217.174.238]

Trace complete.
```

Questions About Paths

Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named traceroute.txt.

1. Is any part of the path common for all hosts you tracerouted?

   Yes, path taken is common.

2. Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?

Yes, the farther the location from my place, more is the number of nodes that appear.

3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

   The latency is dependent on the distance between the two communicating nodes. The relationship hold for all hosts.

Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. *Whois* can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

When using *whois* to look up a domain name, use the simple two-part network name, not an individual computer name (for example, *whois spit.ac.in*).

Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.

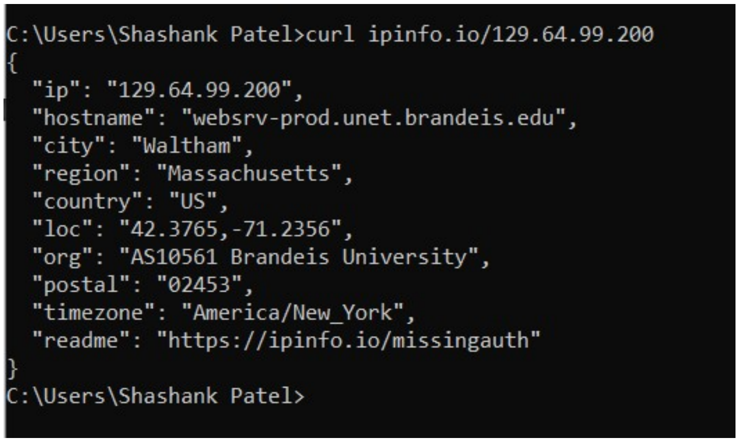
Exercise 5: (Should be short.) Because of NAT, the domain name *spit.ac.in* has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

This geolocation program is not installed on our computers, but you can access one on the command line using the *curl* command, which can send HTTP requests and display the response. The following command uses *curl* to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>. For a specific example:

```
curl  ipinfo.io/129.64.99.200
```

(As you can see, you get back more than just the location.)



```
C:\Users\Shashank Patel>curl ipinfo.io/129.64.99.200
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3765,-71.2356",
  "org": "AS10561 Brandeis University",
  "postal": "02453",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\Shashank Patel>
```

Exercise 6: Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.

Conclusion:

I have learnt basic networking utilities like ping,tracert and ipconfig. I studied factors that affect the round trip time and the latency factors.

References:

https://www.keycdn.com/support/what-is-latency

https://blog.stackpath.com/latency/